ePrescribing Data Use Problem Statement

Created by the *ePrescribing Data Use Task Group*
April 1, 2009

Background and Summary

The California Privacy and Security Advisory Board (CalPSAB) was established by the Secretary of the California Health and Human Services Agency (CHHS). The CalPSAB mission is to develop and recommend privacy and security policies for California Health Information Exchange (HIE) that promote quality of care, respect the privacy and security of individual health information, and enhance trust. The CalPSAB's four committees; Privacy, IT Security, Legal, and Education, are responsible for analyzing issues, developing and evaluating the effectiveness of alternative solutions, and presenting recommendations to the CalPSAB.

In November of 2007, as part of the Privacy Committee's work, the Patient Consent for Health Information Exchange (HIE) Task Group was formed with the mission to define and evaluate the alternatives for individual consent to exchange health information in California. The Patient Consent for HIE Task Group advanced in their work with a progressive awareness of the need to place the consent options in context with specific scenarios, one of them being ePrescribing. As each of the task groups toiled through the consent options, growing insight into the need for two significant pieces of information emerged.

One piece that was needed to affirm a consent option was access control standards. It was deemed critically necessary to have the appropriate controls in place to manage access to the data before a patient could consent to the flow of their data in an HIE. The second piece that was needed was an understanding of secondary uses of information in the health care environment. In order to facilitate an HIE founded in privacy it was necessary to understand the flow of the data. Thus, the ePrescribing Data Use Phase II Task Group was constituted in January of 2009.

Methodology

The Use of ePrescribing Data Use Task Group used a collaborative methodology to determine what problems undermine a successful HIE environment that indoctrinates privacy throughout the flow of ePrescribing data. The Task Group represents a collaboration of public and private sector entities that interact with prescribing data as it flows through the health care environment. Included in the Task Group are county, hospital, pharmacy, provider, research, and health plan representatives. One specialty speaker assisted the Task Group with validation of specific data flows in and out of the ePrescribing hub.[1] The ePrescribing Data Use Task Group members included:

- ✓ Deborah Yano-Fong, University of California San Francisco
- ✓ Jennifer Frost, CalRHIO
- ✓ Gail Gannon, Ensante
- ✓ John Macaulay, Anakam
- ✓ David Nelson, San Diego County

[1] Tom Groom, SVP Business Development at SureScripts-RxHub, provided an overview of the ePrescribing Process on February 26, 2009.

- ✓ Teri Miller, Department of Health Care Services
- ✓ Lori Potter, Kaiser
- ✓ Chuck Steen, Catholic HealthCare West
- ✓ Lee Tien, Electronic Frontier Foundation
- ✓ Patrick Robinson, CalPERS
- ✓ Doug Hillblom, Prescription Solutions
- ✓ Vicky Kirby-Martin,
- ✓ Kathleen Delaney-Greenbaum, California Office of Health Information Integrity
- ✓ Staci Goodwin, California Office of Health Information Integrity

Prior to convening as a group, research was compiled to create a preliminary view of the current ePrescribing landscape. The research consisted of information provided on the internet as well as independent interviews with relevant parties. A flow chart was then crafted to illustrate the flow of prescribing data and the entities involved. Once this information was prepared and assembled, the Task Group met using the following methodology:

- ✓ ***Review steps in the data flow*** – Each scenario step in the data flow was reviewed for accuracy in depiction by subject matter experts who represent the entities in the data flow. Missing steps in the flow were added where appropriate and inaccurate steps were corrected or removed from the data flow.

NOTE: Due to lack of task group representation, not all steps in the data flow were validated by individuals who represent an entity in the diagram, specifically, data mining vendors, pharmaceutical companies, and long term care facilities.

- ✓ ***Review purpose of the data flow*** –The purpose of the data use was reviewed at each step in the data flow. Often times, at this point secondary use issues emerged as privacy needs, deficiencies in process, lack of standards, and other problems were discussed.
- ✓ ***Describe relationships for each step in the data flow*** – After each step was addressed for accuracy and purpose of data use, the set(s) of relationships between entities involved in each step of the scenario were reviewed. A step could have one set of relationships defined or multiple relationships depending on the complexity of data flow and the number of entities involved.

- ✓ ***Describe facilitators and barriers to the data flow*** – After the relationships were established, the facilitators and barriers to the flow of data were described. Legal analysis was prepared prior to the Task Group meeting to describe where data was allowed by law or contract to flow and where the data was not allowed to flow.
- ✓ ***Develop Problem Statement*** –The problems in the use of ePrescribing data emerged from the Task Group discussions. A Problem Statement report was created to document each of the issues.

The Task Group acknowledged the newly signed (February 17, 2009) American Recovery and Reinvestment Act (ARRA) that includes provisions associated with privacy and security of health information. The new legislation is loaded with requirements, new enforcement provisions and penalties for covered entities, business associates, vendors and others. Although the Health Information Technology for Economic and Clinical Health Act (HITECH Act) contains these specific provisions, subsequent clarifications and guidance by the federal government still need to be provided. Therefore, the problems addressed in this report were not set against the HITECH Act provisions. Future Task Groups will take a closer examination of the problems and will include HITECH Act provisions as part of the analysis. The information gathered in the ePrescribing Data Use Task Group will be available to those future Task Groups.

Problem Findings

Six distinct problems related to secondary uses of ePrescribing data emerged from the work of the Use of ePrescribing Data Task Group. Those problems are listed as the following:

1. Loose De-identification and Re-identification Rules
2. Secondary Uses of ePrescribing Data by Vendors
3. Inadequate Research Protocols Regarding ePrescribing Data
4. Secondary Uses of ePrescribing Data for Data Mining, Data Aggregation, Data Informatics, Data Warehousing
5. Overly Broad Business Associate Agreement and Data Use Agreement Language
6. Secondary Use of ePrescribing Data by Employers

Loose De-identification and Re-identification Rules

The existing laws around de-identification and re-identification seem to be loosely defined and interpreted and an area of potential risk to the privacy of an individual's prescribing information. The lack of clear standards, as well as oversight of the de-identification of health information process causes potentially significant privacy issues with ePrescribing data that has been deemed "de-identified".

The HIPAA Privacy Rule provides two ways in which information may be de-identified. In the first way, a covered entity must eliminate 18 specific identifiers out of the data. In many cases this is not the option that is chosen due to the need by researchers and other entities for one or more of the identifiers that have been eliminated, such as data of birth. The second way requires that the covered entity use a licensed statistician to ensure that the information is de-identified in a manner that statistically guarantees that the data can not be identified or later re-identified.

A concern arises as seemingly de-identified data becomes re-identified. Although a covered entity may reasonably assure that the data is not re-identifiable, it is all too often that, for example, data mining companies reassemble data from various sources

to recreate identifiable data.[2] Without a clear means to ensure that data is not later re-identified the risk to the privacy of an individual's prescribing information is heightened.

Secondary Uses of ePrescribing Data by Vendors

The appropriate secondary uses of ePrescribing data by vendors seems to be laced with enough ambiguity to instill concern for the privacy of individual's health information. Vendors' use of ePrescribing data for purposes outside of purposes directly related to treatment (i.e., the provider, pharmacy, or hospital) is questionable. For example, it is understood that a provider may outsource his/her practice management system or electronic medical record system to a vendor. The vendor who has access to the provider's patients' information is clearly a business associate. However, there is concern that the data that is being used to run the system could be re-used by the vendor without knowledge by the provider or the patient.[3]

The use of vendors for ePrescribing software and services is a fact of modern day and becoming more prevalent with incentives from the Federal Government. There is no ambiguity in the acceptable use of vendors as business associates according to the HIPAA Privacy Rule. The same goes for the CMIA. It is the secondary uses of the information by the vendors that comes into question. There seems to be blurred lines in how the vendor can or can not use the information. The problem resides in the lack of transparency of the data use by vendors.

Inadequate Research Protocols Regarding ePrescribing Data

The release of ePrescribing data for research purposes by providers, pharmacies, and hospitals provides a rich source of data; however, the Institutional Review Board (IRB) process that surrounds the release of this health information seems inadequate. The IRB is a committee established to review and approve research involving human subjects. As the IRB process is limited to Federal guidance, it needs review to include state-level guidance necessary for the proper safeguarding of health information used in research.

Besides the lack of IRB guidance, the secondary uses of research data eventually become a privacy problem. Data that was intended to be used for research for one purpose may end up being used for an entirely different purpose that lacks transparency to patients and entities that release the data. . Appropriate informed consent on the risks to privacy from secondary releases is a major issue which needs further review.

Another point is that it is difficult to discriminate between "research" and "quality improvement". Generally both the Common Rule and HIPAA regulations consider a project to be human subject research if the primary purpose is to add to generalizable knowledge. The problem is that projects often have dual goals of quality improvement and research. The appropriate use can be blurred by project description and since

---

[2] Porter, Christine. "DE-IDENTIFIED DATA AND THIRD PARTY DATA MINING: THE RISK OF RE-IDENTICATION OF PERSONAL INFORMATION." *Shidler Journal of Law Commerce & Technology*. Sep. 23, 2008. December 17, 2008 <http://www.lctjournal.washington.edu/Vol5/a03Porter.html>.

[3] Parks, Liz. "IMS, Allscripts band together." Drug Store News. March 20, 2000. December 4, 2008 <http://findarticles.com/p/articles/mi_m3374/is_4_22/ai_61492754>.

quality improvement activities do not require IRB approval, the information can be less scrutinized and less protected.

The problem related to research is complex and warrants the creation of a separate Task Group to analyze it in more detail. Among many related research issues is the issue of "informed consent". Until issues of secondary use are resolved it is not clear what would constitute appropriate informed consent. This issue, and other issues, will need to be discussed further in a future Task Group.

Secondary Uses of ePrescribing Data for Data Mining, Data Aggregation, Data Informatics, Data Warehousing

The mining and aggregating of ePrescribing data although good for many purposes can be used for other unintended purposes. Data miners or aggregators who have access to various data sets are able to compile data that is seemingly "anonymyzed" or "de-identified" into identifiable data.[4] As part of this process, it is unclear as to the rules around who is performing the de-identification of the data before it is usable by another entity, or even usable by the same entity that performed the de-identification. The laws and protections of the data are not clearly understood regarding business associates that have access to identifiable data in order to de-identify for a purpose that resides with the covered entity.

Very large data mining companies access and merge data from a multitude of sources to create physician prescribing data that is later used for marketing, promotions, and sales.[5] Typically this is prohibited; however, the same entities that create the physician prescribing data also perform data mining for public health and research that are appropriate uses of the data.[6] The lines of data uses begin to blend and blur eventually and the fact that the entity may not even be considered a covered entity makes it even harder to determine privacy and security implications. The lucrative nature of combined prescription data is sold to various payers, employers, marketing companies, pharmaceutical companies, and researchers by data mining companies.[7]

A covered entity may engage a business associate to perform any of a number of duties on its behalf, including reporting to a public health entity when required by law. The laws that cover this type of release of information allow the disclosure by the business associate.[8] However, it is unclear as to the rules that protect the health information that

---

[4] Porter, Christine. "DE-IDENTIFIED DATA AND THIRD PARTY DATA MINING: THE RISK OF RE-IDENTICATION OF PERSONAL INFORMATION." Shidler Journal of Law Commerce & Technology. Sep. 23, 2008. December 17, 2008 <http://www.lctjournal.washington.edu/Vol5/a03Porter.html>.

[5] "SDI Acquires Verispan." Business Wire. FindArticles.com. 23 Mar, 2009. December 12, 2008 <http://findarticles.com/p/articles/mi_m0EIN/is_2008_July_29/ai_n27952135>.

[6] Steinbrook, Robert M.D. "For Sale: Physicians' Prescribing Data." *New England Journal of Medicine* 2006 354: 2745-2747. November 15, 2008. December 4, 2008 <http://content.nejm.org/cgi/content/full/354/26/2745>.

[7] "IMS Health: Company Information." IMS Health.com. November 18, 2008 <http://www.imshealth.com/portal/site/imshealth/menuitem.a953aef4d73d1ecd88f611019418c22a/?vgnextoid=98d57900b55a5110VgnVCM10000071812ca2RCRD>.

[8] "Wolters Kluwer Health's Unique Prescription Data Tapped by FDA in Effort to Advance Drug Safety." WKHealth.com. November 3, 2008. December 4, 2008

is part of this process. The legal authority for a data mining company to collect massive amounts of information prior to use by public health officials is unclear, as are the secondary uses of the very same data since most data mining companies offer a variety of services from research and public health to sales and marketing[9]. The problem resides in the lack of transparency and unclear data use rules for data mining, data aggregating, and other data analytics type companies.

Overly Broad Business Associate Agreement and Data Use Agreement Language

Much of the individual health information transmitted and shared is done in accordance with agreements and contracts in place for business associates and researchers. There is a concern that the overly broad language in these agreements may legally allow secondary uses of health information that appear to be unintended uses from the original disclosure.

There is concern that the HIPAA Business Associate Agreement language that is intended to inform the business associate partner of their obligation to protect the health information being used on behalf of the covered entity does not refine the restrictions on secondary uses of the information. This lack of specificity allows secondary uses of ePrescribing data for which it was not intended originally. For example, a provider may engage a data mining company as a business associate who aggregates patient data in order to review health outcomes of prescribing certain medications. Depending on how specific the language is in the business associate agreement, it is possible that the information that has been aggregated is then used for other purposes of the business associate.

Business Associate Agreements that lack the details of when a use is appropriate, for what purpose, how much data, for how long, etc… allow secondary uses to occur. Along with broad language is the lack of actual accountability of the business associate. Covered entities rarely have language in their agreements, let alone resources, to oversee and audit their business associates. This leaves a means for which privacy can be unknowingly disregarded.

Data Use Agreements (DUAs) that outline uses of limited data sets fall into the very same category as Business Associate Agreement in their lack of specificity regarding data uses. The DUAs tend to be too general and allow secondary uses to propagate unbeknownst to anyone except the user of the data.

Secondary Use of ePrescribing Data by Employers

Employers seek prescription-related data to help plan for insurance costs and to create health improvement strategies for their employees. Due to the detailed nature of the information that some larger companies receive to manage their costs, it is uncertain as

---

<http://www.wkhealth.com/pt/re/wkhealth/11032008.htm;jsessionid=JHhf0ZhbYG71DD0K8TLHgTZ2GypbznV04lXgQ4Th02XGThJBBkwy!-269263472!181195628!8091!-1>.

[9] "Wolter Kluwer Health – Source." WKHealth.com. January 6, 2009 <http://www.wkhealth.com/pt/re/wkhealth/source.htm;jsessionid=JLqT50L1JGCQWnnyyr1ZmpQyspCQmmy7xnkCTkvTWvVSm5GXgtZG!-256325120!181195629!8091!-1!1238084206974>.

to the degree of "de-identification" that is performed on the data. Knowing an individual's annual health cost, their gender, and their diagnosis leaves room for re-identification of the individual even within a large-sized company.

Employers currently can engage data mining companies to obtain information on prescription use by their employees. Employers have an expectation to see what they are paying for including knowledge of how effectively plans are managing chronic disease and engaging members in services that improve the health of their employees. There is pressure by larger companies to obtain more detailed health data, including prescription information.[10]

The level of data seems more aggregated than de-identified and causes concern for the privacy of individuals. The problem resides with the lack of transparency to the employee/patient who does not know the employer is reviewing their prescription information. The information in the hands of the employer can be seen as a positive look into obtaining better care for employees, but it also becomes worrisome as it would not be evident if an employee was dismissed from their job due to health care costs.

Conclusion

Secondary use and re-use of health data is becoming a rapidly escalating issue. As California continues in the direction of HIE adoption, more electronic health data will become readily available and more and more entities will want to access and use these data for multiple purposes. The Use of ePrescribing DataTask Group discovered six distinct areas of privacy concern when looking specifically at secondary uses of ePrescribing data including de-identification and re-identification problems, vendor concerns, inadequate research protocol, data mining issues, broad contract language, and secondary uses by employers.

The secondary uses of ePrescribing data serve a multitude of purposes including public good. Unfortunately, with lack of clear guidelines for the uses and re-uses of ePrescribing data mentioned in this document, problems with the privacy of individuals' information will continue to surface with increasing speeds in an HIE. These problems require closer examination in order to tweeze out legitimate secondary uses from inappropriate secondary uses, as well as to specify limitations on those uses of ePrescribing data.

NOTE: Two issues that were not addressed in this report, but were revealed during the Task Group's work were 1) lack of enforcement of the current HIPAA Privacy and Security Rules and 2) the lack of rules regarding the Master Patient Index. These issues are important; however, they are unrelated to the scope of the Use of ePrescribing Data Task Group which addresses secondary uses. Those two issues will be examined as part of the overarching issues related to all pieces of a health information exchange in the work being completed by the Legal Committee.

[10] Skernivitz, Stephanie. "Where Data Stops: Employers want more data for cost planning, but where is line drawn?" Managed HealthCare Executive. June 1, 2008. December 17, 2008 <http://managedhealthcareexecutive.modernmedicine.com/mhe/Special+Report/Where-Data-Stops-Employers-want-more-data-but-wher/ArticleStandard/Article/detail/522497>.

Next Steps

The intent of the Task Group's *Use of ePrescribing Data Problem Statement Report* is to support the next phases of secondary use work. In concert with the Problem Statement Reports from the Lab Data Use Task Group, Emergency Department Task Group, Public Health Task Group, Mental Health Task group, Telemedicine Task Group, and Personal Health Record Task Group, this report will be assimilated into a single view that lists and prioritizes all of the secondary use problems.

It is assumed that each Task Group will generate its own set of problems for the specific scenario they are examining. Where there are overlaps in problems, there will be a harmonization of the issue in order to avoid duplicative efforts. A joint task group will then be assembled to explore a deeper understanding of each of the secondary use problems, including a closer look at the purpose of the data use, the limitations of its use, the privacy interests of those using the data, and the harms that may occur to an individual whose data is being used. Ultimately, the group will construct alternatives to resolving each of the problems.